**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

| | | |
|---|---|---|
| Southwestern Bell Telephone Company; AT&T Communications of Texas, Inc.; Indiana Bell Telephone Company d/b/a AT&T Indiana; Pacific Bell Telephone Company d/b/a AT&T California; BellSouth Telecommunications, LLC; Teleport Communications Group, Inc. d/b/a TCG Illinois; New Cingular Wireless PCS, LLC d/b/a AT&T Mobility; and SNET Diversified Group, Inc. d/b/a AT&T Diversified Group, | ) | |
| Plaintiffs, | ) | |
| v. | ) | Civil Action No. 3:11-cv-02009-O |
| Phil Iverson; Chris J. Gose; Feature Films for Families, Inc.; All Things Family, Inc.; CCI Communications LLC; Blue Skye, L.C.; Vera, L.C.; and **John Does 1-50** | ) | |
| Defendants. | ) | |

**PLAINTIFFS' FIRST AMENDED COMPLAINT**

Southwestern Bell Telephone Company d/b/a AT&T Kansas, AT&T Missouri, and AT&T Texas ("Southwestern Bell"); AT&T Communications of Texas, Inc.; Indiana Bell Telephone Company d/b/a AT&T Indiana ("AT&T Indiana"); Pacific Bell Telephone Company d/b/a AT&T California ("AT&T California"); BellSouth Telecommunications, LLC d/b/a/ AT&T Georgia, AT&T North Carolina, and AT&T Tennessee ("BellSouth"); Teleport Communications Group, Inc. d/b/a TCG Illinois ("TCG Illinois"); New Cingular Wireless PCS, LLC d/b/a AT&T Mobility ("AT&T Mobility"); and SNET Diversified Group, Inc. d/b/a AT&T Diversified Group ("AT&T DG") (all Plaintiffs are collectively referred to as "AT&T" or the "Plaintiffs"), hereby file this Complaint for fraud, trespass, conversion, unjust enrichment,

violation of the federal Computer Fraud and Abuse Act ("CFAA"), 18 USC § 1030, and other statutory causes of action arising under state law against Defendants Phil Iverson ("Iverson"); Chris J. Gose ("Gose"); Feature Films for Families, Inc. ("Feature Films"); All Things Family, Inc. ("ATF"); CCI Communications LLC ("CCI"); Blue Skye, L.C. ("Blue Skye"); Vera, L.C. ("Vera"); and John Does 1-50 (collectively, the "Defendants"), alleging on personal knowledge as to AT&T, and on information and belief as to all other matters, as follows:

## NATURE OF THE CASE

1. Over at least the past five years, defendants have repeatedly and deliberately abused AT&T's telecommunications network by engaging in multiple acts of fraud and deception to misappropriate private and commercially valuable customer data from AT&T's computer database.

2. Defendants have accomplished their data theft by using auto-dialing programs to make hundreds of millions of "spoofed" telephone calls to telephone lines that Defendants have purchased from AT&T in Texas and other states. These spoofed calls replace the Defendants' calling party numbers with telephone numbers assigned not to the Defendants, but to other wireline and wireless telephone service subscribers, many of whom are AT&T customers.

3. The purpose of these spoofed calls is to trick AT&T's electronic telephone switches (which are specialized types of computers) and related network facilities into searching for, and delivering to the Defendants, Caller ID name and number information for hundreds of millions of telephone numbers stored in AT&T's electronic customer name ("CNAM") database and other CNAM databases.

## BACKGROUND

4. AT&T maintains an electronic CNAM database that matches North American telephone numbers issued to AT&T (by the North American Numbering Plan Administrator) with the name of the AT&T subscribers to whom AT&T assigns those numbers. This information has considerable commercial value, particularly given the increasing number of wireless service subscribers and hence wireless telephone numbers, for which matching name and number information is generally not available through published directories, directory assistance, or other public information sources.

5. Since 2006, the Defendants – at the direction of Defendants Iverson and Gose – have repeatedly used deception and fraud to trespass on AT&T's telecommunications network, gain unauthorized access to AT&T's CNAM database, and "harvest" commercially valuable subscriber name and number information that belongs to AT&T and is stored in AT&T's CNAM database. This database has substantial commercial value to AT&T, because it provides, on a linked basis, customer telephone numbers and customer names, which for many customers – wireless customers in particular – is not available to Defendants on a consolidated basis through commercial directory services. Defendants have regularly modified their "*modus operandi*" to try to conceal their data mining from AT&T, and have repeatedly lied to AT&T about the nature of their activities. Upon information and belief, Defendants have improperly obtained such AT&T subscriber information to illegitimately further their own business interests, likely including but not limited to the provision of telemarketing services, either by Defendants or entities with whom Defendants have business relationships.

6. To carry out their data theft, various Defendants purchase telecommunications services, including multi-line services, from AT&T (and other telecommunications providers) at

locations around the country. One of the services Defendants purchase is caller identification with name ("Caller ID") service. When purchased by a called party, Caller ID service generally allows the called party to see the name and number of the calling party.

7. Each of the fraudulently spoofed calls causes the AT&T computerized switching facilities associated with the called phone lines to generate an electronic Caller ID inquiry into the appropriate electronic CNAM database, thereby causing AT&T's network systems to provide its Caller ID customer (the called party – here one of the Defendants) with the name of the person or entity associated with the phone number of the calling party. In a split-second, through several hardware and software functions contained in AT&T's network, the queried CNAM database matches each spoofed calling number with the name of the person or entity to whom the number has been assigned (the "subscriber") and sends that information to the called party. Because Defendants are on both sides of these calls – initiating and receiving them – they are able (on the calling side) to use computerized auto-dialing functions to spoof millions of calling numbers for which Defendants seek CNAM data, and then (on the receiving end) to capture the customer name information displayed on their Caller ID devices.

8. Defendants' unlawful data mining has imposed significant costs on AT&T – including not only the network-related costs of processing hundreds of millions of spoofed telephone calls, but also the costs and fees associated with the CNAM data searches themselves (which are charged for on a "per-dip" basis by the CNAM database providers) and the costs of detecting, uncovering, and taking steps to reduce the recurrence of, the fraud. In addition, because of its commercial value, Defendants likely have used the misappropriated CNAM data for telemarketing and/or other commercially valuable purposes. Since 2006, AT&T's internal network fraud detection organization has uncovered numerous instances of Defendants' data

mining schemes. In some cases, AT&T has terminated or disabled the services that Defendants have used to accomplish their unlawful data mining; in other cases, Defendants themselves have stopped using their AT&T services once the fraud has been detected.

9. But even when they abandon one service, Defendants' data mining continues – in new locations, using different telephone lines, different services, and even different carriers. By constantly adjusting and refining their data mining techniques, Defendants have been able to launch a series of cyber-attacks on and gain unauthorized access to AT&T's electronic CNAM database during the past 5 years.

10. Defendants' fraudulent and deceptive abuse of AT&T's network to steal CNAM data constitutes fraud, trespass, conversion, and a violation of the CFAA as well as numerous state laws, and has unjustly enriched the Defendants.

## JURISDICTION AND VENUE

11. This Court has jurisdiction to resolve all claims asserted in this Complaint. This Court has diversity jurisdiction under 28 U.S.C. § 1332, because this is a civil action between citizens of different states, and the amount in controversy exceeds the sum or value of $75,000. In addition, pursuant to 28 U.S.C. § 1331, this Court has subject matter jurisdiction over Count XXXVIII, which asserts a claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and the Court has supplemental jurisdiction over the remaining claims pursuant to 28 U.S.C. § 1367.

12. Venue in this district is proper under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims asserted in this Complaint occurred in this district. This Court has personal jurisdiction over each Defendant because each Defendant resides, may be found, has an agent, or transacts his or its affairs in this district.

## PARTIES

### Plaintiffs

13. As set forth more specifically in Paragraphs 14 – 21 below, each of the Plaintiffs is a direct or indirect subsidiary of AT&T Inc., a publicly-held Delaware corporation with its principal place of business in Dallas, Texas. Certain of the Plaintiffs are local exchange carriers ("LECs") that have provided local exchange telecommunications services to the Defendants, which Defendants have abused to accomplish their unlawful data mining. In addition, the AT&T LECs own much of the CNAM data that Defendants have stolen from AT&T's CNAM database. Defendants' data mining has imposed significant costs on the AT&T LECs, including the network-related costs of processing hundreds of millions of spoofed telephone calls, the "per-dip" costs of the resulting Caller ID searches of AT&T's CNAM database and the CNAM databases of other CNAM data warehouse providers, and the costs of developing and deploying additional network-related hardware and software to better enable AT&T to detect and take corrective action against Defendants' fraudulent activity. Defendants also have been unjustly enriched by their unlawful data mining activities, which have enabled Defendants to obtain, for no additional cost beyond the cost of the services they purchased from AT&T, commercially valuable directory information of millions of AT&T subscribers that, but for Defendants' misconduct, either would not be obtainable by Defendants at all (in the case of AT&T wireless service subscribers' directory information) or would be obtainable by Defendants only at a substantially greater cost (in the case of AT&T wireline service subscribers' directory information). All told, Defendants' unlawful conduct has caused AT&T to suffer damages in excess of $6,500,000.

14. Plaintiff Southwestern Bell is a Missouri corporation with its principal place of business in Dallas, TX. Southwestern Bell does business in a 5-state region in the Southwestern United States. This action involves data mining in three Southwestern Bell States: Kansas, Missouri, and Texas. In Kansas, Southwestern Bell does business as "AT&T Kansas." In Missouri, Southwestern Bell does business as "AT&T Missouri." In Texas, Southwestern Bell does business as "AT&T Texas." AT&T Kansas, AT&T Missouri, and AT&T Texas are each ILECs in their authorized service areas in Kansas, Missouri, and Texas respectively, and each is also a telecommunications service provider that provides local exchange telecommunications service in Kansas, Missouri, and Texas, respectively. Defendants have misused telecommunications services purchased from AT&T Kansas, AT&T Missouri, and AT&T Texas in their data mining schemes.

15. Plaintiff AT&T Communications of Texas, Inc. is a Delaware corporation with its principal place of business in Dallas, Texas. AT&T Communications of Texas is a telecommunications service provider that is certificated to provide, and is providing, local exchange telecommunications and other telecommunications service in Texas. Defendants have misused telecommunications services purchased from AT&T Communications of Texas in their data mining schemes.

16. Plaintiff TCG Illinois is a Delaware corporation with its principal place of business in Bedminster, New Jersey. TCG Illinois is a telecommunications service provider that is certificated to provide, and is providing, local exchange telecommunications and other telecommunications services in Illinois. Defendants have misused telecommunications services purchased from TCG Illinois in their data mining schemes.

17. Plaintiff AT&T Indiana is an Indiana corporation with its principal place of business in Indianapolis, Indiana. AT&T Indiana is an ILEC in its authorized service areas in Indiana and provides local exchange telecommunications service in the state of Indiana. Defendants have misused telecommunications services purchased from AT&T Indiana in their data mining schemes.

18. Plaintiff AT&T California is a California corporation with its principal place of business in San Francisco, California. AT&T California is an ILEC in its authorized service areas in California and provides local exchange telecommunications service in the state of California. Defendants have misused telecommunications services purchased from AT&T California in their data mining schemes.

19. Plaintiff BellSouth is a Georgia limited liability company with its principal place of business in Atlanta. BellSouth does business in a 9-state region in the Southeastern United States. This action involves data mining in three BellSouth states: Georgia, North Carolina, and Tennessee. In Georgia, BellSouth does business under the name "AT&T Georgia." In North Carolina, BellSouth does business under the name "AT&T North Carolina." In Tennessee, BellSouth does business under the name "AT&T Tennessee." AT&T Georgia, AT&T North Carolina, and AT&T Tennessee are each ILECs in their authorized service areas in Georgia, North Carolina, and Tennessee, respectively. Each is also a telecommunications service provider that provides local exchange telecommunications services in Georgia, North Carolina, and Tennessee, respectively. Defendants have misused telecommunications services purchased from AT&T Georgia, AT&T North Carolina, and AT&T Tennessee in their data mining schemes.

20. Plaintiff AT&T Mobility is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. AT&T Mobility provides wireless

telecommunications services throughout the United States, and the names and numbers of AT&T Mobility's customers are stored in AT&T's electronic CNAM database and have been a prime target of Defendants' data mining.

21. Plaintiff AT&T DG is a Connecticut corporation with its principal place of business in New Haven, CT. AT&T DG maintains and provides an electronic CNAM database for AT&T and manages the CNAM information of the AT&T LECs and other carriers, including AT&T Mobility, who store their CNAM information on that database. AT&T DG offers services, for a fee, that use its electronic CNAM data base. These services include a name and number verification service, which is used by many vendors as a form of identification in connection with certain types of credit card and online commercial transactions, among other things. AT&T DG is also the assignee of claims by the AT&T ILECs and CLECs whose customer name and number data was mined from the AT&T CNAM database by the Defendants.

**Defendants**

22. The Defendants (other than Iverson and Gose) are a group of inter-related entities – many of whom are corporations with minimal assets – that Iverson and Gose have directed or caused to engage in certain unlawful data mining activities, as further described below.

23. Defendant Phil Iverson ("Iverson") is an individual residing in Utah. In his dealings with AT&T, Iverson has held himself out to be an agent or employee of Defendants CCI Communications, Feature Films for Families, and Blue Skye, among others, authorized to act on their behalf, and has signed agreements to purchase telecommunications services from certain of the Plaintiffs on behalf of CCI Communications, Feature Films For Families, and Blue Skye. Iverson has caused the corporate defendants to misuse AT&T's telecommunications network by engaging in repeated acts of CNAM data mining. Iverson also has lied to AT&T

about the nature of CCI's and Feature Films' activities, in an effort to conceal Defendants' unlawful data mining from AT&T.

24. Defendant Chris J. Gose ("Gose") is a co-founder, officer, and employee of Defendant CCI Communications LLC. He resides in Utah. Gose has directed and controlled the activities of certain of the entity Defendants and knowingly facilitated and participated in the Defendants' misuse of AT&T's telecommunications network by engaging in repeated acts of CNAM data mining. Gose has made misrepresentations to AT&T about the nature of CCI's and Feature Films' activities. In addition, Gose has represented to AT&T that Iverson has authority to act for CCI.

25. Defendants Iverson and Gose are referred to herein as the "Individual Defendants."

26. Defendant Feature Films is a Utah corporation with its principal place of business at 5286 Commerce Drive, Murray, Utah 84107. Feature Films is a producer and telemarketer of PG- and G-rated family films, and operates a number of telemarketing call centers around the United States. Feature Films places solicited and unsolicited telephone sales calls to market its film products. Feature Films purchases telecommunications products and services from communications providers, including AT&T. Feature Films sometimes does business under the name "Blue Skye."

27. Defendant ATF is a Utah corporation with its principal place of business at 5286 Commerce Drive, Murray, Utah 84107, the same address as Feature Films. ATF also has the same registered agent (Matthew G. Cooper, 5286 Commerce Drive, Ste A116) and many of the same officers and directors as Feature Films.

28. Defendant CCI is a Delaware limited liability corporation with its principal place of business at 155 N. 400 W. Suite 100, Salt Lake City, Utah 84103. CCI is owned, dominated and controlled by the Individual Defendants. CCI provides communications services to end users, including Feature Films, and to resellers of communications services, acts as a consultant to such resellers and end-users, including Feature Films, and has purchased services from AT&T that enable CCI to furnish those services to Feature Films.

29. Defendant Blue Skye is a Utah limited liability company with its principal place of business at 5282 Commerce Drive, Murray, Utah 84107, within the same office building complex as Feature Films and ATF. "Blue Skye" is also the name under which Feature Films has purchased telecommunications services from Plaintiffs in Illinois.

30. Defendant Vera is a Utah limited liability company with its principal place of business at 5282 Commerce Drive, Murray, Utah 84107, the same address as Blue Skye. Vera also has the same registered agent (Russell D. Harris, 5282 Commerce Drive, Ste D292) and the same manager (Katerina Pollack, 5282 Commerce Drive, Ste A116) as Blue Skye.

31. Defendants Blue Skye and Vera each used the same billing address to order telecommunications services from AT&T: P.O. 30204, Salt Lake City, UT 84130. This is also the same billing address used by Defendant ATF on several of its accounts, for which Defendant Iverson was listed as the customer contact and authorized representative.

32. Each of Defendants Feature Films, ATF, CCI, Blue Skye, and Vera (i) does business in Texas, (ii) has purchased telecommunications services from AT&T in Texas and other states, and (iii) has used those services to defraud AT&T, trespass on its telecommunications network, gain unauthorized access to AT&T's electronic CNAM database, and steal valuable proprietary CNAM data from AT&T.

33. John Does 1 through 50 are Defendants who are currently unknown or have not yet been identified. Their names will be added as their identities become known.

## GENERAL ALLEGATIONS

### The North American Numbering Plan, Caller ID, and Caller Name ("CNAM") Databases

34. Telephone numbers in the United States are issued in accordance with the North American Numbering Plan ("NANP"), an integrated numbering system for the United States, Canada, Bermuda, and certain Caribbean countries. Under the NANP, every telephone number in the United States consists of ten digits: a three-digit numbering plan area code ("NPA"), a three-digit central office exchange code ("NXX"), and a four-digit subscriber number or "station code." There are hundreds of millions of telephone numbers in the NANP system. The NANP Administrator, currently NeuStar, Inc., issues telephone numbers, usually in blocks of 10,000 sequential numbers, to certified telecommunications carriers through a written request process initiated by the carrier.

35. When a carrier assigns an NANP telephone number to a subscriber, that telephone number is associated with that subscriber's name and is stored in an electronic CNAM database. CNAM databases are used to match customer names and numbers for purposes of providing Caller ID information, among other things. CNAM databases are subsets of more comprehensive electronic "Line Information Databases," which include address and other information about the subscriber, and are maintained by a number of telecommunications carriers and other service providers in the United States, including AT&T DG, Verizon, Qwest, TNS, and Embarq.

36. Every time a telephone call is made in North America, it is transmitted to the receiving customer's telephone line by a series of electronic routing computers, each of which is

known as a "switch", and associated network facilities connected to those switches. Telecommunications carriers (like the AT&T LECs) that provide local exchange and exchange access telecommunications services maintain switches in their local service areas to route the calls made to, and from, their local exchange service customers. When a call is placed to a party that subscribes to Caller ID, the network switch serving the receiving customer (*i.e.*, the called party) briefly suspends the call, marks it with a "tag," and launches an electronic CNAM query to identify the customer name associated with the calling party number. When the receiving customer is on the AT&T network (as the Defendants have been), the applicable AT&T switch serving that customer initiates the CNAM query. If the queried number is in AT&T's own CNAM database, the calling party customer name is electronically retrieved from that database and the information is sent back to the switch serving the receiving customer, which matches the information with the "tagged" call and displays the information on the receiving customer's Caller ID device. If the queried number is not in AT&T's database, the query is re-routed to the appropriate external electronic CNAM database (such as Verizon's or Qwest's), and the calling party customer name (up to a maximum of 15 characters) is electronically retrieved and sent back to the switch serving the receiving customer for display on the Caller ID device.

37. Although it involves several hardware and software functions, the average CNAM query takes only about 500 milliseconds to complete – less than the time it takes for a telephone to ring twice. The search can be completed, and the Caller ID information can be displayed, even if the call is not completed (*i.e.*, answered); indeed, one function of Caller ID service is to allow the called party to identify callers before answering the phone.

**AT&T's CNAM Database**

38. AT&T DG, a member of the AT&T corporate family, maintains and manages a computer database of subscriber names associated with wireline and wireless telephone numbers assigned to those subscribers by AT&T. In addition, AT&T DG stores subscriber name and telephone number information for certain other telecommunications carriers, under contract with AT&T DG. AT&T's CNAM database is located in Connecticut, and the data it contains is the property of the various telecommunications carriers (such as Plaintiffs Southwestern Bell, AT&T Mobility, and BellSouth) whose subscriber name and number information is stored in the database.

39. AT&T's CNAM database contains commercially valuable private information, including the identity and telephone numbers of AT&T Mobility's wireless subscribers, in a format that is not otherwise easily available, and is a significant asset of AT&T.

40. CNAM queries cause the AT&T LECs to incur a variety of costs, including, among others, the following: (i) the switching and transport-related costs of processing each incoming call onto AT&T's network; (ii) the cost of using AT&T's internal processing capacity to initiate a CNAM query for each call; (iii) the fees charged by AT&T DG – the manager of AT&T's database – to each AT&T LEC for each query performed on data in AT&T's CNAM database (other than the AT&T LEC's own data); and (iv) the fees charged to each AT&T LEC by third party CNAM data warehouse providers for searches of their CNAM databases when the calling party number is assigned to a carrier whose CNAM information is not stored on the AT&T database. If the incoming call is placed from an AT&T switch, AT&T incurs additional costs, including call setup charges.

**The Mechanics of Call "Spoofing" and CNAM "Data Mining"**

41. The basic requirement for a data mining scheme is the purchase of telephone services that (i) provide multiple telephone lines that allow the party to make and receive a large number of automated calls; (ii) allow the party to hide or replace the party's own calling party number with another, "spoofed," number, so the party can make calls that appear to be coming from someone else; (iii) allow the party making the calls to receive the calls; and (iv) allow the calling party to capture the information displayed on the called party's Caller ID device.

42. Among the services that AT&T and other telecommunication carriers offer is an Integrated Services Digital Network/Primary Rate Interface service (commonly known as "PRI" service). PRI is a voice and data service that provides high-volume access to the public switched telephone network ("PSTN") facilities of the PRI service provider/carrier. A customer that purchases a PRI service can have as many as 24 voice lines for each PRI, and can have multiple PRIs – meaning hundreds of telephone lines – at one location. The customer can dedicate some of the PRI lines to outgoing calls, and the rest to incoming calls. Or the customer can dedicate all of the lines to outgoing or incoming calls. Calls from one line on the PRI can be made to another line of the PRI, thus enabling a PRI customer to call itself from one PRI line to another at a single location.

43. Although the carrier providing the PRI service will assign to the customer purchasing the PRI up to 24 telephone numbers for each PRI purchased, PRI service also enables the purchaser of the service to use commercially available software to customize the calling party number ("CPN") to whatever number the purchaser chooses. This is most typically (and appropriately) used when the calling party (usually a business or office) has multiple assigned numbers but wants a single main "business" number (and name) to appear on a called party's

Caller ID device. This makes it easier for a customer to return a call, or to identify who is calling before answering.

44. But the ability to customize the calling party number can be abused: it is possible for a purchaser of PRI service to hide or replace its own calling party number with a number that has not been assigned to that purchaser. There is no legitimate reason for a PRI purchaser to hide or replace its true calling party number with a telephone number that has no relationship to that purchaser to make it appear that the call is coming from someone else.

45. "CNAM data mining" refers to the misuse of telephone services, including PRI service, to make a large number of short-duration or "ring-no-answer" (also known as "no-duration") telephone calls that hide the calling party's true ten-digit calling party number by overlaying other ten-digit telephone numbers not assigned to the calling party (the "spoofed CPNs") in order to collect (or "harvest") the customer names (CNAMs) associated with the spoofed CPNs. With the use of auto-dialing computer programs, a single end user with multiple telephone lines (like those provided by AT&T's PRI service) can make tens of millions of spoofed telephone calls in a matter of days. This activity is now prohibited by federal law under the Truth In Caller ID Act of 2009, Pub. Law No. 111-331.

46. While some of Defendants' data mining schemes used a single PRI purchased from AT&T for both outgoing and incoming calls, Defendants have continually adapted their schemes to avoid – or delay – detection. For example, after AT&T discovered that Defendants were calling themselves on a single AT&T PRI, AT&T disabled Defendants' ability to spoof telephone calls that they originated through the AT&T PRI service. Defendants responded by simply calling their AT&T PRI lines from telephone lines (including PRIs) that Defendants purchased from other carriers. In addition, rather than sending all the data mining calls to a

single PRI, Defendants made their data mining calls to "plain old telephone service" ("POTS") end-user lines they had purchased from AT&T. They also stopped using large blocks of sequential telephone numbers for their "spoofing" activities, relying instead on randomly-generated numbers that would not appear in numerical order in AT&T's call detail records. In all cases, AT&T has detailed calling records that demonstrate Defendants' conduct as further described below. AT&T will make these records available to Defendants in accordance with Fed. R. Civ. P. 26 or in response to a properly framed discovery request.

## DEFENDANTS' ACTS OF DATA MINING

47. Set forth below are each of the principal acts of data mining that AT&T has identified to date. Because the Defendants have made substantial efforts to conceal their data mining activities, AT&T may not have discovered all of Defendants' acts of data mining.

### Defendants' Data Mining in Utah (2006)

48. By agreement dated October 22, 2004, Iverson, on behalf of Feature Films, executed a one-year agreement with ACC Business, an affiliate of TCG Utah acting on behalf of TCG Utah, under which Feature Films purchased an AT&T PRI service called "PrimePlex." Feature Films was assigned 20 telephone numbers: 801-290-4250 (the main Billing Telephone Number, or "BTN") through 4269. That agreement was extended for another one-year term on August 23, 2005, in another contract signed by Iverson on behalf of Feature Films. In both agreements, Iverson was listed as Feature Films' "IT Manager."

49. On or about August 23, 2005, Defendant Iverson caused Feature Films to enter into a "Master Agreement" with AT&T Corp. (reference no. 3001275), acting on behalf of TCG Utah, to purchase additional PRI service in Salt Lake City, Utah.

50. The AT&T PRI services that Iverson purchased from TCG Utah gave Feature Films access to multiple telephone lines in Utah.

51. In May 2006, AT&T detected approximately 3 million automated, "no-duration" calls ("no-duration" calls are calls that are not answered by a person or a machine) being received by two of the AT&T PRIs that Feature Films had purchased from TCG Utah. The BTNs for those PRIs were 801-290-4250 and 801-905-4421. The calls originated from PRI service that Feature Films had purchased from Qwest (another local exchange carrier in Utah). None of the 3 million calls was answered. Each call was immediately followed by another call, originating from the same Qwest PRI and using a different spoofed number.

52. The high volume of ring-no answer calls received by Feature Films and the calling pattern of those calls led AT&T's internal network fraud organization to conclude that Feature Films likely was engaged in CNAM data mining in violation of Section 3.2.1 of TCG Utah's state tariff, which prohibited use of the services offered by AT&T "for any unlawful purpose "; indeed, there was no other plausible explanation for the observed calling activity.

53. Robert Gorman of AT&T contacted Defendant Iverson by telephone on June 9, 2006 to inquire about the high volume of short-duration calls that Feature Films was receiving on its two Utah PRIs. Iverson admitted that Feature Films had been calling itself, and said that Feature Films had been "testing" certain equipment used in Feature Films' telemarketing. Iverson assured Gorman that the testing had stopped and that AT&T would no longer see this type of activity on Feature Films' PRIs.

54. However, despite Iverson's representation that the alleged equipment "testing" had stopped, the high volume of short-duration calling activity by Feature Films to its AT&T PRIs in Utah continued.

55. Exercising its rights under the TCG Utah tariff, AT&T notified Feature Films, by letter dated June 12, 2006 to Feature Film's registered agent and lawyer, Matthew Cooper, that

"the manipulation of AT&T services [by masking the true CPN that had placed the call with another number] is an unauthorized and inappropriate use of [AT&T's network and services]." AT&T informed Feature Films that if the CNAM data mining did not stop within 24 hours, AT&T would terminate Feature Films' services.

56. Gorman then spoke with Iverson again, on June 13, 2006. This time, Mr. Gorman was joined by Adam Panagia, the Associate Director of AT&T's Network Fraud Investigations group. Iverson agreed to allow AT&T to remove the Caller ID with name function from Feature Films' Utah PRIs. The data mining activity then stopped, and shortly thereafter Feature Films discontinued its AT&T PRI service in Utah.

**Defendants' First Dallas Data Mining Scheme (2006 – 2007)**

57. By agreement dated September 15, 2006, Iverson, acting on behalf of CCI, purchased eight AT&T PRI lines in Dallas, Texas on an expedited basis from AT&T Communications of Texas, Inc. CCI requested the activation of 80 telephone lines on these PRIs at a single Dallas location; these lines were assigned telephone numbers 469-221-1900 (main BTN) through 1979, and were then made available by CCI (or in Gose's own words, "supplied by" CCI) to Feature Films. Between November 20, 2006 and July 26, 2007, Defendants caused more than 21 million calls to be made to Defendants' Dallas PRI service. All of these calls originated on Defendants' Dallas PRI service. In other words, Defendants used the Dallas PRI service purchased from AT&T to call themselves 21 million times. Each of these calls had a unique "spoofed" CPN, which was unrelated to the 80 telephone numbers assigned to Defendants' PRI service. The calls were made in a sequential NPA/NXX pattern. The calls lasted an average of 6 seconds each. Each of these calls generated a CNAM query, which revealed the name of the subscriber to whom each "spoofed" CPN was assigned.

58. The unusual calling pattern and call volumes strongly suggested to AT&T that either CCI or one of its co-Defendants was intentionally generating fraudulent CNAM queries: the tens of millions of "spoofed" sequential calling party numbers were neither assigned to, nor had any relationship with, CCI (or any other Defendant), and those calls could have no legitimate purpose.

59. In a July 10, 2007 telephone conversation with Iverson, Adam Panagia of AT&T told Iverson that AT&T had again observed a pattern of misuse of AT&T's network for CNAM data mining. Iverson stated that CCI was acting as an agent and circuit provider for Feature Films for Families, and that the traffic pattern was due to "call transfers" of inbound call activity to outbound survey calls. Panagia told Iverson that this explanation was not consistent with the fact that the calls lasted only 6 seconds on average and that the calling party numbers followed a sequential pattern. Iverson then changed his story, telling AT&T that The Dove Foundation, a charitable organization based, on information and belief, in Grand Rapids, Michigan, provided CCI with blocks of numbers to confirm as active telephone numbers prior to a telemarketing campaign.

60. Later that same day, Iverson, Gose, Forrest Baker (the owner of Feature Films), Greg Cope (who worked for CCI in the area of Operations) and Mike Bills (a vice-president of Feature Films) called Adam Panagia of AT&T. Panagia informed Iverson, Gose and the others that their deceptive calling activity was an unauthorized use and violation of AT&T's network and services and constituted a theft of proprietary CNAM data; as a result, Panagia told Defendants that delivery of Caller ID with name information would be suspended immediately for the Dallas PRIs.

61. On or about July 19, 2007, AT&T blocked CCI's ability to "spoof" CPNs for outgoing telephone calls from its Dallas PRIs, except for those numbers within the 80-number range assigned to CCI.

62. Once CCI could no longer spoof CPNs not assigned to it, the unusual calling activity on the Dallas PRIs stopped, at least temporarily.

63. On July 24, 2007, Iverson contacted the AT&T network maintenance and repair organization and reported as trouble on CCI's Dallas PRIs the inability to freely substitute CPNs on those PRIs. Without disclosing CCI's and Feature Film's prior telephone discussions with Mr. Panagia, Iverson requested that this trouble be repaired. Following its normal procedures, the AT&T network maintenance and repair organization opened a customer help ticket to have CCI's CPN substitution (or spoofing) capabilities reinstated on the Dallas PRIs. An AT&T service technician mistakenly reset the feature, allowing CCI to resume spoofing CPNs.

64. Two days later, on July 26, 2007, AT&T's Panagia noticed over 10,000 calls transmitted over the CCI Dallas PRI circuits starting at around 8:15 a.m. Once again, AT&T disabled the CPN substitution feature on those PRI circuits for CPNs not assigned to CCI, and the suspicious calling activity stopped.

65. In November 2007, Iverson contacted AT&T and asked to have CCI's CPN substitution ability restored on the CCI Dallas PRI lines. In an email dated November 2, 2007, Iverson told Panagia that "Feature Films is doing some legitimate service bureau work" and "would like the ability to send Caller ID again. Can they have this feature turned back on?" Iverson signed this email as "CCI Telecom Manager." AT&T did not reactivate this feature on the Dallas PRI lines.

**Defendants' Second Dallas Data Mining Scheme (2008)**

66. During 2008, AT&T noticed the same pattern of unusual calling activity and call volumes on certain terminating CCI PRI circuits (PRI circuits receiving inbound calls) in AT&T's Dallas network that AT&T had observed in 2006 and 2007. The calling pattern strongly suggested that either CCI or one of its co-Defendants was intentionally generating CNAM queries: the millions of spoofed sequential calling party numbers terminating on those PRI lines neither were assigned to, nor had any relationship with, CCI.

67. Since Defendants could no longer spoof calls originating on their Dallas PRIs, Defendants used a third party carrier's PRI service to initiate the data mining calls; but the calls were still made ***to*** CCI's Dallas PRIs. By continuing to call itself, CCI ensured that it would control the Caller ID devices on which the harvested CNAM data would be displayed.

68. By using a carrier other than AT&T to launch its unauthorized and unlawful data mining assault into AT&T's network and AT&T's electronic CNAM database, Defendants made it more difficult for AT&T to detect their data mining.

69. This change in Defendants' *modus operandi* demonstrates that Defendants knew that their data mining was an unauthorized and fraudulent misuse of AT&T's network and services.

70. From April 2008 through June 2008, Defendants caused more than 22 million calls – again using sequentially-numbered CPNs – to be made to CCI's AT&T PRIs in Dallas from telephone lines Defendants had purchased from a third-party carrier. These calls had an average duration of 1.36 seconds. As with Defendants' other data mining schemes, each call generated a CNAM query, linking the sequentially-numbered CPN with the name of the subscriber to whom the CPN was assigned.

71. In June 2008, AT&T disabled CCI's Caller ID with name feature on the Dallas PRIs. CCI subsequently requested that its Dallas PRI service be terminated, and AT&T did so in July 2008.

72. By letter dated September 19, 2008, AT&T notified Defendant Gose of CCI's unlawful calling activity and demanded reimbursement of AT&T's costs incurred as a result of CCI's abuse of the AT&T network. AT&T calculated that CCI's data mining schemes had caused it to incur over $650,000 in CNAM query charges and related network expenses: $90,401 due to CCI's initial data mining activity on its Dallas PRIs, $93,084 due to CCI's subsequent data mining activity on those PRIs, and $473,465 due to data mining activity that AT&T had recently discovered on PRI lines that CCI had obtained in Atlanta, Georgia (see Paragraphs 74 – 78). In an effort to resolve the dispute, however, AT&T only demanded reimbursement for its base CNAM query charges, which totaled approximately $529,400.

73. The Defendants, however, continued to deny that they were engaged in data mining, and did not reimburse AT&T.

**Defendants' Atlanta Data Mining Scheme (Dec. 2006 – Sept. 2008)**

74. By agreements dated August 23, 2006 and December 5, 2006, Defendant Iverson, on behalf of CCI, purchased from AT&T Georgia eight "PRI Advantage Plus" lines with Caller ID. The lines were assigned eight different BTNS (all sharing the same NPA/NXX of 404-870): 2026, 3910, 1760, 1090, 2300, 1648, and 8150. Iverson specifically requested that AT&T remove the "Screening Tables" from CCI's PRI services, a software feature that prevented call spoofing on this particular type of PRI service.

75. Using the PRI services that Iverson purchased on its behalf, CCI made more than 112,000,000 calls to its AT&T Georgia PRIs from November 2006 to September 2008, using sequentially-numbered, spoofed CPNs, each of which generated a CNAM query.

76. The calling pattern and call volumes strongly suggested that CCI was intentionally generating CNAM queries: the millions of spoofed, sequential calling party numbers neither were assigned to, nor had any relationship with, CCI.

77. This fraudulent and unauthorized use of AT&T's network and resulting unauthorized access of AT&T's electronic CNAM database violated Section A2.2.9 of BellSouth's General Subscriber Service Tariff (the "AT&T Georgia Tariff"), which states that service is provided on the condition that it not be used for an unlawful purpose.[1] Moreover, section A2.2.10.A.7.a. of the AT&T Georgia Tariff provides that AT&T may cancel service or terminate a subscriber's contract due to abusive or fraudulent conduct.

78. Upon discovering the fraud in July 2008, AT&T notified CCI of the misuse of AT&T's network and services, and of CCI's breach of tariff. CCI thereafter terminated its AT&T PRI services in Georgia.

**Defendants' Chicago Data Mining (Feb 2008 – Mar 2009 )**

79. By agreement dated June 14, 2007, Defendant Iverson, on behalf of Defendant Feature Films "d/b/a Blue Skye," purchased from TCG Illinois PrimePlex PRI services with 40 telephone lines at 111 N. Canal St., Chicago (main BTN 312-777-4505), for use in Illinois, pursuant to TCG Illinois' tariff – TGC Illinois IL C.C. No. 3.

80. Between February and June 2008, Feature Films made over 4.3 million calls to its Chicago PRI lines using spoofed CPNs. Feature Films made each of these calls from one of its

[1] See http://cpr.bellsouth.com/pdf/ga/g001.pdf

Chicago PRIs to another, under an apparent belief that its billing arrangement provided for unlimited local calling. However, under Feature Films' contract, originating local calls on the Chicago PRI lines were charged a fee for the first 18 seconds of use and for every six second increment thereafter. Thus, Feature Films incurred substantial local usage charges on its Chicago PRI lines through June 2008.

81. After receiving the bill for these charges, Defendant Iverson disputed the amounts Feature Films owed, claiming that Feature Films was entitled to unlimited local calling. However, instead of ceasing its data mining activity, Defendants simply began placing calls to Feature Films' Chicago PRIs from telephone lines provided by other carriers, including XO Communications, to avoid incurring AT&T's local usage charges for originating calls. By March 2009, Defendants had made an additional 1.2 million calls to Feature Films' Chicago PRI lines from telephone lines provided by third party carriers.

82. Eventually, after AT&T made clear to Iverson that Feature Films' Chicago PRI lines would not enjoy free, unlimited local calling for originating calls and that AT&T was monitoring the highly unusual calling activity and call patterns involving those lines, Feature Films ceased using its Chicago PRI lines and making payments against the charges it owed.

**Feature Films' Qwest Data Mining Scheme (2008)**

83. In October 2008, AT&T discovered significant data mining activity originating from a switch in Salt Lake City, Utah that belonged to Qwest Communications, a telecommunications service provider operating throughout several western states. AT&T observed over 50,000 CNAM queries launched from this switch during a single 24-hour period.

84. Shortly after AT&T informed Qwest of the suspicious traffic (and accompanying CNAM queries) originating from Qwest's switch, Qwest traced the querying activity to PRIs on

its network that Defendant Iverson had obtained on behalf of Feature Films. Feature Films was once again calling itself, but using PRIs that it purchased from Qwest. Just as AT&T had done in Utah and Dallas on the PRIs that Feature Films and CCI, through Defendant Iverson, had purchased from AT&T in those locations, Qwest removed the Caller ID feature on the Qwest PRIs to prevent Feature Films from engaging in further data mining.

**Vera's Tennessee Data Mining (2010)**

85. During June 2010, AT&T discovered that Defendant Vera, a subscriber to AT&T's local telephone service in Franklin, Tennessee, was engaging in fraudulent calling activity and data mining using the following telephone numbers (all sharing the same NPA/NXX of 615-771): 5650 (main BTN), 5145, 5193, 5228, 5376, 5385, 5614, 5692, 5814, 5817, 5853, and 5881. Additional numbers were later discovered registered to Vera (BTN: 615-292-2677) in Nashville, Tennessee.

86. Between March and June 2010, Defendants made over 2 million calls to Vera's telephone numbers associated with BTN 615-771-5650 and over 1.5 million calls to Vera's telephone numbers associated with BTN 615-292-2677, each of which generated a resulting CNAM query.

87. AT&T disconnected the service due to Vera's fraudulent use of AT&T's network in violation of the applicable BellSouth tariff, as well as Section 6(c) of the AT&T Business Services Agreement, which prohibits the unlawful use of retail telecommunications service or abuse of AT&T's network.[2]

88. In an email exchange with M. Myrick of AT&T dated June 11 and 12, 2010, Michael Starkey of QSI Consulting, Inc., who purported to be acting on behalf of Defendant

[2] *See* http://www.corp.att.com/agreement/docs/serviceagreement_2009.pdf.

Vera , asserted that the termination was "unlawful," and that there was, to his knowledge, no "tariff language that prohibits [Defendants'] use of the [AT&T] service in the way they have used it." In response, AT&T explained that the lines had been disconnected

> because your client has been using them to data-mine CNAM information by "spoofing" the CPNs to obtain the actual subscribers' names. We have determined that over 100,000,000 calls have been placed to exchange services purchased by your client since the start of the year with the calling party number replaced to enable the capture of the name and telephone number of unrelated third parties.

Mr. Starkey responded by stating that his "client" did not believe that it had violated any tariff, or had broken the law, and he said that he would recommend that his client bring a complaint at the Tennessee PUC. The services were not restored, and no complaints were filed at the PUC.

**Defendants' Additional Acts of Data Mining (2008 – 2010)**

89. Defendants have continued to engage in data mining at various locations around the country, using telephone service purchased from AT&T and other carriers. The calling pattern and call volumes, described chronologically below, can only be explained as part of a coordinated, intentional, and ongoing effort to make data mining calls using spoofed telephone numbers so Defendants can discover the names associated with those numbers and create their own CNAM database.

90. Between December 2008 and June 2010, over 14 million calls were received by 8 telephone lines purchased from AT&T by Defendant ATF and terminating at ATF's facilities located at 17304 Preston Road, Ste 800, Dallas, TX 75252. Defendant ATF also purchased from AT&T the Caller ID with name feature for each of these 8 telephone lines. The BTN at this location was 972-248-4123. These calls lasted an average of approximately 3 seconds each.

91. Between December 2008 and June 2010, nearly 20 million telephone calls – each lasting only a few seconds – were received by 8 telephone lines purchased (along with the Caller

ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 100 Highland Park Shopping Village, Ste 200, Highland Park, TX 75205. The billing telephone number ("BTN") at this location was 214-520-7201. These calls lasted an average of approximately 2 seconds each.

92. Between January 2009 and June 2010, approximately 20.5 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 5100 Westheimer, Ste 200, Houston, TX 77056. The BTN at this location was 713-963-0584. These calls lasted an average of approximately 4 seconds each.

93. Between January 2009 and June 2010, more than 9 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 7500 College Blvd., 5th Floor, Lighton Tower, Overland Park, KS 66210. The BTN at this location was 913-339-9348. These calls lasted an average of approximately 5.5 seconds each.

94. Between March 2009 and June 2010, more than 16 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 5847 San Felipe St., Floor 17, Houston, TX 77057. The BTN at this location was 713-334-2151. These calls lasted an average of 4.5 each.

95. Between April 2009 and June 2010, nearly 14 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 7500 College Blvd., 5th Floor,

Lighton Tower, Overland Park, KS 66210. The BTN at this location was 913-345-9537. These calls lasted an average of approximately 4.75 seconds each.

96. Between May 2009 and June 2010, nearly 9 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 1200 Smith, Floor 16, Two Allen Center, Houston, TX 77002. The BTN at this location was 713-651-1012. These calls lasted an average of approximately 5.7 seconds each.

97. Between January and June 2010, approximately 5.5 million telephone calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 3180 Irving Blvd., Dallas, TX 75247. The BTN at this location was 214-905-1201. These calls lasted an average of approximately 2.7 seconds each.

98. Between January and June 2010, more than 5 million telephone calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 5100 Westheimer Rd., Ste 200, Houston, TX 77056. The BTN at this location was 713-622-7607. These calls lasted an average of approximately 5 seconds each.

99. Between January and June 2010, more than 4 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 1200 Smith, Floor 16, Two Allen Center, Houston, TX 77002. The BTN for this location was 713-651-1107. These calls lasted an average of approximately 6 seconds each.

100. Between February and June 2010, nearly 5 million calls were received by 7 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 5847 San Felipe St., Floor 17, Houston, TX 77057. The BTN at this location was 713-781-0794. These calls lasted an average of approximately 6 seconds each.

101. Between February and June 2010, nearly 2 million calls were received by 11 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 1200 Abernathy Road, Ste 1700, Sandy Springs, GA 30328. The BTN at this location was 770-671-9127. These calls lasted an average of approximately 8 seconds each.

102. Between March 2009 and June 2010, nearly 2 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 2015 Ayrsley Town Blvd., Suite 202, Charlotte, NC 28273. The BTN at this location was 704-504-5833. These calls lasted an average of approximately 5.8 seconds each.

103. Between March and June 2010, approximately 1.5 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 6000 Fairview Rd., Suite 1200, Charlotte, NC 28210. The BTN at this location was 704-551-4116. These calls lasted an average of approximately 6.7 seconds each.

104. Between March and June 2010, nearly 2 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 301 McCullough

Drive, Charlotte, NC 28262. The BTN at this location was 704-595-9340. These calls lasted an average of approximately 6.75 seconds each.

105. Between March and June 2010, approximately 1.5 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 3003 Summit Blvd., 14th Floor, Atlanta, GA 30319. The BTN at this location was 404-257-1387. These calls lasted an average of approximately 7.5 seconds each.

106. Between March and June 2010, more than 2 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 450 E. 96th Street, Ste 500, Indianapolis, IN 46240. The BTN at this address was 317-580-0531. These calls lasted an average of approximately 5.7 seconds each.

107. Between March and June 2010, more than 2 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 8888 Keystone CRSG, Ste 1300, Indianapolis, IN 46240. The BTN at this location was 317-581-8949. These calls lasted an average of approximately 6 seconds each.

108. Between March and June 2010, more than 2 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 201 N. Illinois Street, 16th Floor, Indianapolis, IN 46204. The BTN at this location was 317-635-8607. These calls lasted an average of approximately 6 seconds each.

109. Between January and June 2010, more than 11.5 million calls were received by 8 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant ATF and terminating at ATF's facilities located at 2300 Main, 9th Floor, Kansas City, MO 64108. The BTN at this location was 816-559-9202. These calls lasted an average of approximately 5 seconds each.

110. Between March and June 2010, more than 1 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Vera's facilities located at 425 Market, Ste 2200, San Francisco, CA 94105. The BTN at this location was 415-908-3800. These calls lasted an average of approximately 8 seconds each.

111. Between March and June 2010, approximately 1.5 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 4370 La Jolla Village Dr., Ste 400, San Diego, CA 92122. The BTN at this location was 858-458-1002. These calls lasted an average of approximately 5.8 seconds each.

112. Between March and June 2010, more than 1 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities also located at 4660 La Jolla Village Dr, Ste 500, San Diego, CA 92122. The BTN at this location was 858-642-1900. These calls lasted an average of approximately 6.7 seconds each.

113. Between March and June 2010, more than 1 million calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Blue Skye and terminating at Blue Skye's facilities located at 402 W. Broadway,

Ste 400, San Diego, CA 94133. The BTN at this location was 619-544-1800. These calls lasted an average of approximately 6.7 seconds each.

114. Between March and June 2010, approximately 670,000 calls were received by 12 telephone lines purchased (along with the Caller ID with name feature for each line) from AT&T by Defendant Vera and terminating at Blue Skye's facilities located at 301 Clay, Ste 500, San Francisco, California 94111. The BTN at this location was 415-397-2100. These calls lasted an average of approximately 5.25 seconds each.

**FRAUDULENT CONCEALMENT**

115. In an effort to conceal their unlawful data mining activity from AT&T, Defendants have (i) used different corporate entities to contract with, and/or purchase services from, different AT&T local exchange carriers and AT&T service resellers in different locations around the country, (ii) concealed the interrelationships of the various Defendants, (iii) misrepresented the nature of their activities when directly questioned about them by AT&T, (iv) changed the manner in which they conduct their data mining by initiating the mining calls from facilities that Defendants purchase from carriers other than AT&T and spreading the receiving telephone lines (the called telephone numbers) for the data mining calls among various telephone lines the Defendants have purchased from AT&T, which makes it much more difficult for AT&T to detect the unlawful calling activity, and (v) carried out data mining schemes entirely on other carriers' networks while still using "spoofed" CPNs that belonged to AT&T subscribers, making it impossible for AT&T to stop Defendants from data mining simply by terminating their services.

**DEFENDANTS' ILLEGAL DATA MINING IS LIKELY TO CONTINUE UNLESS ENJOINED BY THIS COURT.**

116. Since 2006, AT&T has detected numerous instances of Defendants' data mining and fraudulent and unauthorized telephone calling activity using AT&T's network and services, has demanded that Defendants stop their unlawful, unauthorized, and fraudulent activities, and has terminated or disabled the particular services that Defendants have used for their unauthorized and illegal activities. But notwithstanding the evidence demonstrating their culpability, Defendants have consistently denied that they are engaged in unauthorized and unlawful data mining, and have refused to acknowledge and discontinue it. Indeed, Defendants are not deterred even when their service is terminated or disabled: Defendants have simply stopped using or paying for AT&T services once their ability to engage in data mining has been compromised. Defendants have used their various interrelated corporate entities to purchase new and different services from which to both launch and obtain the unlawful fruits of their data mining, which, on information and belief, continues unabated.

117. Although the named corporate Defendants, to the best of AT&T's knowledge, have stopped purchasing services directly from AT&T to accomplish their data mining, it is possible – if not probable – that Defendants will continue to engage in similar schemes under different guises, or use other carriers' services to launch unauthorized data mining attacks on AT&T and unlawfully invade AT&T's network facilities and steal information from AT&T's electronic CNAM database, as they have already done. The AT&T electronic CNAM database is constantly revised and updated as new telephone numbers are issued and assigned to relocated or new subscribers, and as old telephone numbers are returned by departing subscribers and re-assigned to other subscribers. As a result, Defendants need to continue their data mining of AT&T's electronic CNAM database to keep their own unlawfully-obtained, mirror database

"current." Otherwise, Defendant's "mirrored" database would quickly become outdated and of limited use to them. Thus, there can be little question that Defendants intend to, and will, continue their data mining unless and until they are enjoined from doing so by this Court.

118. Indeed, Defendants' use of various networks and carriers to deliver data mining calls to the AT&T PRIs and ordinary AT&T telephone lines purchased by Defendants, as described above, demonstrates that Defendants intend to continue their illegal, fraudulent, and unauthorized data mining activity and are deliberately trying to avoid detection of such continued activity.

**COUNT I**
**FRAUD – TEXAS COMMON LAW**

119. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 118 above as if fully set forth herein.

120. Under Texas law, it is unlawful to make a material representation with knowledge of its falsity and with the intent to induce reliance in another, where such representation is actually and justifiably relied upon, thereby resulting in injury.

121. To carry out their data mining scheme in Texas, Defendants made millions of material false representations by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

122. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to induce AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

123. AT&T actually and justifiably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of

each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

124. AT&T has been injured as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

125. AT&T has suffered damages in excess of $365,000 as a result of the conduct described in Count I.

**COUNT II**
**FRAUD – ILLINOIS COMMON LAW**

126. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 125 above as if fully set forth herein.

127. Under Illinois law, it is unlawful to make a knowingly false statement of material fact, intended to induce another to act, where such statement is relied upon by another and damages result from such reliance.

128. To carry out their data mining scheme in Illinois, Defendants made millions of false statements of material fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

129. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to induce AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

130. AT&T actually and justifiably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of

each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

131. AT&T has suffered damages as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

132. AT&T has suffered damages in excess of $13,000 as a result of the conduct described in Count II.

**COUNT III**
**FRAUD – GEORGIA COMMON LAW**

133. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 132 above as if fully set forth herein.

134. Under Georgia law, it is unlawful to make a false representation or omission of a material fact with knowledge of its falsity, intended to induce another to act or refrain from acting, where such statement is justifiably relied upon, thereby resulting in damages.

135. To carry out their data mining scheme in Georgia, Defendants made millions of misrepresentations of existing material fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

136. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to induce AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

137. AT&T actually and justifiably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of

each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

138. AT&T has suffered damages as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

139. AT&T has suffered damages in excess of $285,000 as a result of the conduct described in Count III.

**COUNT IV**
**FRAUD – TENNESSEE COMMON LAW**

140. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 139 above as if fully set forth herein.

141. Under Tennessee law, it is unlawful to make an intentional and knowing misrepresentation of an existing material fact which causes another's reasonable reliance and resulting damages.

142. To carry out their data mining scheme in Tennessee, Defendants made millions of material false representations of existing fact by intentionally overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

143. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to induce AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

144. AT&T actually and reasonably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid CPN of

each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

145. AT&T has suffered damages as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

146. AT&T has suffered damages in excess of $8,000 as a result of the conduct described in Count IV.

**COUNT V**
**FRAUD BY MISREPRESENTATION – KANSAS COMMON LAW**

147. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 146 above as if fully set forth herein.

148. Under Kansas law, it is unlawful to knowingly make an untrue statement of fact with the intent to deceive another, where such statement is reasonably relied and acted upon to the innocent party's injury.

149. To carry out their data mining scheme in Kansas, Defendants made millions of false statements of fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

150. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to deceive AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

151. AT&T actually and reasonably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed")

CPN of each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

152. AT&T has been injured as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

153. AT&T has suffered damages in excess of $56,000 as a result of the conduct described in Count V.

**COUNT VI**
**FRAUD – INDIANA COMMON LAW**

154. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 153 above as if fully set forth herein.

155. Under Indiana law, it is unlawful to knowingly make a material misrepresentation of existing fact which causes another's reliance and resulting detriment.

156. To carry out their data mining scheme in Indiana, Defendants made millions of material misrepresentations of existing fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

157. Defendants knew that the CPN data embedded in their outgoing calls was false.

158. AT&T was induced to act in reliance upon Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

159. AT&T has been injured as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

160. AT&T has suffered damages in excess of $17,000 as a result of the conduct described in Count VI.

**COUNT VII**
**FRAUD – CALIFORNIA COMMON LAW**

161. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 160 above as if fully set forth herein.

162. Under California law, it is unlawful to make a knowing misrepresentation of fact with intent to induce another's reliance, where such misrepresentation is justifiably relied upon to the innocent party's detriment.

163. To carry out their data mining scheme in California, Defendants made millions of material false representations of fact by intentionally overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

164. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to induce AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

165. AT&T actually and justifiably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid CPN of each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

166. AT&T has been injured as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

167. AT&T has suffered damages in excess of $14,000 as a result of the conduct described in Count VII.

**COUNT VIII**
**FRAUD – MISSOURI COMMON LAW**

168. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 167 above as if fully set forth herein.

169. Under Missouri law, it is unlawful to knowingly make a false representation of material fact within the intent to induce another's reliance, where such misrepresentation is believed and justifiably relied upon, and proximately causes injury to the innocent party.

170. To carry out their data mining scheme in Missouri, Defendants made millions of false statements of material fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

171. Defendants knew that the CPN data embedded in their outgoing calls was false, and intended to deceive AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

172. AT&T actually and reasonably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

173. AT&T has been injured as a proximate result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

174. AT&T has suffered damages in excess of $28,000 as a result of the conduct described in Count VIII.

**COUNT IX**
**FRAUD – NORTH CAROLINA COMMON LAW**

175. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 174 above as if fully set forth herein.

176. Under North Carolina law, it is unlawful to make a false representation or a concealment of a material fact to another, reasonably calculated and made with the intent to deceive, which does in fact deceive another, thereby resulting in injury.

177. To carry out their data mining scheme in North Carolina, Defendants made millions of false statements of material fact by overlaying the CPN data on each outgoing call to match that of another telephone subscriber, including other AT&T customers, when in fact that subscriber was not the true calling party.

178. Defendants knew that the CPN data embedded in their outgoing calls was false, and made an intentional and calculated effort to deceive AT&T into launching CNAM queries of false CPNs upon the belief that they were the true calling party numbers.

179. AT&T actually and reasonably relied on Defendants' misrepresentations. AT&T's switched telephone network initiated a CNAM query based on the overlaid ("spoofed") CPN of each call and returned the corresponding subscriber's Caller ID information as shown in the CNAM database.

180. AT&T has been injured as a result of its reliance on these misrepresentations. For each call, AT&T incurred network costs initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting CNAM query as well as fees charged by the manager of the particular CNAM database queried.

181. AT&T has suffered damages in excess of $12,000 as a result of the conduct described in Count IX.

**COUNT X**
**TRESPASS TO CHATTEL – TEXAS COMMON LAW**

182. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 181 above as if fully set forth herein.

183. Under Texas law, it is unlawful to interfere wrongfully with the use or possession of another's property.

184. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

185. To carry out their data mining scheme in Texas, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

186. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

187. AT&T has suffered damages in excess of $365,000 as a result of the conduct described in Count X.

**COUNT XI**
**TRESPASS TO CHATTEL – ILLINOIS COMMON LAW**

188. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 187 above as if fully set forth herein.

189. Under Illinois law, it is unlawful to cause, with or without physical force, an injury to or interference with another's rightful possession of personal property.

190. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

191. To carry out their data mining scheme in Illinois, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's rightful use and possession of its property.

192. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

193. AT&T has suffered damages in excess of $13,000 as a result of the conduct described in Count XI.

**COUNT XII**
**TRESPASS TO CHATTEL – GEORGIA COMMON LAW**

194. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 193 above as if fully set forth herein.

195. Under Georgia law, it is unlawful to interfere with or damage the personal property of another without authorization.

196. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

197. To carry out their data mining scheme in Georgia, Defendants unlawfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

198. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

199. AT&T has suffered damages in excess of $285,000 as a result of the conduct described in Count XII.

**COUNT XIII**
**TRESPASS TO CHATTEL – TENNESSEE COMMON LAW**

200. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 199 above as if fully set forth herein.

201. Under Tennessee law, it is unlawful to use or intermeddle with personal property in the possession of another.

202. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

203. To carry out their data mining scheme in Tennessee, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

204. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

205. AT&T has suffered damages in excess of $8,000 as a result of the conduct described in Count XIII.

**COUNT XIV**
**TRESPASS TO CHATTEL – KANSAS COMMON LAW**

206. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 205 above as if fully set forth herein.

207. Under Kansas law, it is unlawful to use or intermeddle with personal property in the possession of another.

208. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

209. To carry out their data mining scheme in Kansas, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

210. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

211. AT&T has suffered damages in excess of $56,000 as a result of the conduct described in Count XIV.

**COUNT XV**
**TRESPASS TO CHATTEL – INDIANA COMMON LAW**

212. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 211 above as if fully set forth herein.

213. Under Indiana law, it is unlawful to use or intermeddle with personal property in the possession of another.

214. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization

of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

215. To carry out their data mining scheme in Indiana, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

216. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

217. AT&T has suffered damages in excess of $17,000 as a result of the conduct described in Count XV.

**COUNT XVI**
**TRESPASS TO CHATTEL – CALIFORNIA COMMON LAW**

218. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 217 above as if fully set forth herein.

219. Under California law, it is unlawful to intentionally and without authorization interfere with another's right to possess personal property, where such interference proximately causes damage to the property.

220. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

221. To carry out their data mining scheme in California, Defendants intentionally and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's right to use and possess its property.

222. Such interference has directly caused injury to AT&T's property. AT&T has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

223. AT&T has suffered damages in excess of $14,000 as a result of the conduct described in Count XVI.

**COUNT XVII**
**TRESPASS TO CHATTEL – MISSOURI COMMON LAW**

224. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 223 above as if fully set forth herein.

225. Under Missouri law, it is unlawful to intentionally and without justification intermeddle with a chattel in the possession of another.

226. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

227. To carry out their data mining scheme in Missouri, Defendants intentionally and without justification placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

228. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

229. AT&T has suffered damages in excess of $28,000 as a result of the conduct described in Count XVII.

**COUNT XVIII**
**TRESPASS TO CHATTEL – NORTH CAROLINA COMMON LAW**

230. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 229 above as if fully set forth herein.

231. Under North Carolina law, it is unlawful to dispossess or interfere with property in the possession of another without authorization.

232. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

233. AT&T rightfully possessed this property when Defendants initiated their data mining scheme in North Carolina.

234. To carry out their data mining scheme in North Carolina, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries based on this false CPN data, thereby substantially interfering with AT&T's use and possession of its property.

235. As a result, AT&T has suffered injury to its property. It has incurred additional usage costs associated with initiating and processing both the defendants' "spoofed" CPN

telephone call and the resulting fraudulent CNAM queries, and it has incurred fees charged by the managers of the various CNAM databases that have been queried.

236. AT&T has suffered damages in excess of $12,000 as a result of the conduct described in Count XVIII.

**COUNT XIX**
**CONVERSION – TEXAS COMMON LAW**

237. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 236 above as if fully set forth herein.

238. Under Texas law, it is unlawful to wrongfully exercise dominion and control over another's property in denial of or inconsistent with the true owner's rights.

239. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

240. To carry out their data mining scheme in Texas, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby exercising dominion and control over AT&T's property for their own use and benefit.

241. Defendant's wrongful exercise of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

242. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM

database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

243. AT&T has suffered damages in excess of $2,555,000 as a result of the conduct described in Count XIX.

**COUNT XX**
**CONVERSION – ILLINOIS COMMON LAW**

244. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 243 above as if fully set forth herein.

245. Under Illinois law, it is unlawful to wrongfully assume control or ownership over the personal property of another.

246. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

247. AT&T has an unconditional and immediate right to possess this property.

248. To carry out their data mining scheme in Illinois, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby asserting dominion and control over AT&T's property for their own use and benefit.

249. Defendant's wrongful assumption of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

250. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM

database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

251. AT&T has suffered damages in excess of $100,000 as a result of the conduct described in Count XX.

**COUNT XXI**
**CONVERSION – GEORGIA COMMON LAW**

252. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 251 above as if fully set forth herein.

253. Under Georgia law, it is unlawful to wrongfully or without authorization exercise the right of ownership, dominion, or appropriation over the personal property of another.

254. AT&T owns and has a right to possess its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

255. To carry out their data mining scheme in Georgia, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby asserting dominion and control over AT&T's property and appropriating it to their own use and benefit.

256. Defendant's wrongful exercise of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

257. Defendant's wrongful assertion of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

258. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

259. AT&T has suffered damages in excess of $2,088,000 as a result of the conduct described in Count XXI.

**COUNT XXII**
**CONVERSION – TENNESSEE COMMON LAW**

260. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 259 above as if fully set forth herein.

261. Under Tennessee law, it is unlawful to appropriate another's property to one's own use and benefit, by the intentional exercise of dominion over it, in defiance of the true owner's rights.

262. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

263. To carry out their data mining scheme in Tennessee, Defendants intentionally and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby

exercising dominion and control over AT&T's property and appropriating it to their own use and benefit.

264. Defendant's wrongful exercise of dominion and control over AT&T's property continued for a substantial period of time and was in defiance of AT&T's rights in the property.

265. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

266. AT&T has suffered damages in excess of $66,000 as a result of the conduct described in Count XXII.

**COUNT XXIII**
**CONVERSION – KANSAS COMMON LAW**

267. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 266 above as if fully set forth herein.

268. Under Kansas law, it is unlawful to assume or exercise without authorization the right of ownership over personal property of another to the exclusion of the other's rights.

269. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

270. To carry out their data mining scheme in Kansas, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby

exercising a right ownership over AT&T's property by appropriating it to their own use and benefit.

271. Defendant's wrongful exercise of ownership and control over AT&T's property continued for a substantial period of time and was to the exclusion of AT&T's own rights in the property.

272. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of ownership and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

273. AT&T has suffered damages in excess of $417,000 as a result of the conduct described in Count XXIII.

**COUNT XXIV**
**CONVERSION – INDIANA COMMON LAW**

274. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 273 above as if fully set forth herein.

275. Under Indiana law, it is unlawful to knowingly or intentionally exert unauthorized control over the property of another.

276. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

277. To carry out their data mining scheme in Indiana, Defendants intentionally and without authorization placed millions of calls on AT&T's network embedded with false CPN

data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby asserting control over AT&T's property for their own use and benefit.

278. Defendant's wrongful exercise of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

279. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

280. AT&T has suffered damages in excess of $129,000 as a result of the conduct described in Count XXIV.

**COUNT XXV**
**CRIMINAL CONVERSION – INDIANA CODE § 34-24-3-1**

281. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 280 above as if fully set forth herein.

282. Indiana law provides a private right of action on behalf of victims of criminal conversion. Ind. Code § 34-24-3-1. Under Indiana law, a person commits criminal conversion if he knowingly or intentionally exerts unauthorized control over property of another person. *Id.* § 35-43-4-3.

283. A person may "exert control over property" by possessing it. *Id.* § 35-43-4-1.

284. A person's control over property of another person is "unauthorized" if it is exerted by creating or confirming a false impression in the other person. *Id.*

285. Defendants' conversion of AT&T's switched telephone network, as described in Count XXIV, constitutes criminal conversion in violation of the Indiana Penal Code.

286. AT&T has suffered damages in excess of $129,000 as a result of the conduct described in Count XXV.

287. Under Indiana law, AT&T is entitled to treble damages, costs, and reasonable attorney's fees resulting from Defendants' conversion of its switched telephone network. *Id.* § 34-24-3-1.

**COUNT XXVI**
**CONVERSION – CALIFORNIA COMMON LAW**

288. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 287 above as if fully set forth herein.

289. Under California law, it is unlawful to willfully and without lawful justification interfere with another's right to possess personal property.

290. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

291. AT&T has an unconditional and continuing right to possess this property.

292. To carry out their data mining scheme in California, Defendants wrongfully and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby interfering with AT&T's right to possess and control its property.

293. Defendant's wrongful exercise of dominion and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

294. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of dominion and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

295. AT&T has suffered damages in excess of $107,000 as a result of the conduct described in Count XXVI.

**COUNT XXVII**
**CONVERSION – MISSOURI COMMON LAW**

296. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 295 above as if fully set forth herein.

297. Under Missouri law, it is unlawful to assume and exercise, without authorization, ownership and control over the personal property of another to exclusion of the owner's rights.

298. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

299. AT&T has an unconditional and immediate right to possess this property.

300. To carry out their data mining scheme in Missouri, Defendants intentionally and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby exercising ownership and control over AT&T's property for their own use and benefit.

301. Defendant's wrongful exercise of ownership and control over AT&T's property continued for a substantial period of time and was inconsistent with AT&T's rights in the property.

302. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of ownership and control over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

303. AT&T has suffered damages in excess of $210,000 as a result of the conduct described in Count XXVII.

**COUNT XXVIII**
**CONVERSION – NORTH CAROLINA COMMON LAW**

304. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 303 above as if fully set forth herein.

305. Under North Carolina law, it is unlawful to assume and exercise, without authorization, the right of ownership or dominion over goods or personal property belonging to another, to the exclusion of the owner's rights.

306. AT&T has a property right in its switched telephone network, which includes buildings, equipment, wires, and computers. AT&T also has a property right in the organization of its subscribers' telephone numbers in a single database and the ability to match CPNs with their corresponding subscribers' name and related information.

307. To carry out their data mining scheme in North Carolina, Defendants intentionally and without authorization placed millions of calls on AT&T's network embedded with false CPN data and caused AT&T's equipment to perform CNAM queries of false CPN data, thereby asserting a right of ownership and dominion over AT&T's property for their own use and benefit.

308. Defendant's wrongful exercise of ownership and dominion over AT&T's property continued for a substantial period of time and was to the exclusion of AT&T's rights in the property.

309. As a result, Defendants are liable to AT&T for the full value of their wrongful exercise of ownership and dominion over AT&T's property and misappropriation of the CNAM database, as well as the costs and fees incurred by AT&T in initiating and processing millions of fraudulent CNAM queries.

310. AT&T has suffered damages in excess of $95,000 as a result of the conduct described in Count XXVIII.

**COUNT XXIX**
**UNJUST ENRICHMENT – TEXAS COMMON LAW**

311. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 310 above as if fully set forth herein.

312. Under Texas law, no person may retain a benefit to the loss of another against the fundamental principles of justice or equity and good conscience.

313. Defendants' data mining activity in Texas has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

314. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

315. Defendants have not appropriately compensated AT&T for providing this benefit.

316. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $2,189,000.

**COUNT XXX**
**UNJUST ENRICHMENT – ILLINOIS COMMON LAW**

317. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 316 above as if fully set forth herein.

318. Under Illinois law, no person may retain a benefit to the detriment of another in violation of fundamental principles of justice, equity and good conscience.

319. Defendants' data mining activity in Illinois has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

320. AT&T did so to its own detriment, incurring network usage costs as well as millions of fees charged by the managers of the various CNAM databases that were queried.

321. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

322. Defendants have not appropriately compensated AT&T for providing this benefit.

323. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $86,000.

**COUNT XXXI**
**UNJUST ENRICHMENT – GEORGIA COMMON LAW**

324. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 323 above as if fully set forth herein.

325. Under Georgia law, no person may retain a benefit conferred by another which equitably ought to be returned or adequately compensated for.

326. Defendants' data mining activity in Georgia has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

327. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

328. Defendants have not appropriately compensated AT&T for providing this benefit.

329. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $1,802,000.

**COUNT XXXII**
**UNJUST ENRICHMENT – TENNESSEE COMMON LAW**

330. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 329 above as if fully set forth herein.

331. Under Tennessee law, no person may retain a benefit knowingly received from another under such circumstances as would make it inequitable for the conferee to retain the benefit without payment of its value.

332. Defendants' data mining activity in Tennessee has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

333. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

334. Defendants have not appropriately compensated AT&T for providing this benefit.

335. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $57,000.

**COUNT XXXIII**
**UNJUST ENRICHMENT – KANSAS COMMON LAW**

336. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 335 above as if fully set forth herein.

337. Under Kansas law, no person may retain a benefit knowingly received from another under such circumstances as would make it unjust for the conferee to retain the benefit without payment of its value.

338. Defendants' data mining activity in Kansas has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

339. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

340. Defendants have not appropriately compensated AT&T for providing this benefit.

341. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $361,000.

**COUNT XXXIV**
**UNJUST ENRICHMENT – INDIANA COMMON LAW**

342. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 341 above as if fully set forth herein.

343. Under Indiana law, no person may retain a measurable benefit from another under circumstances in which retention of the benefit without payment would be unjust.

344. Defendants' data mining activity in Indiana has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

345. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

346. Defendants have not appropriately compensated AT&T for providing this benefit.

347. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $111,000.

**COUNT XXXV**
**CLAIM FOR RESTITUTION – CALIFORNIA COMMON LAW**

348. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 347 above as if fully set forth herein.

349. Under California law, no person should be permitted unjustly to enrich himself at the expense of another, but should be required to make restitution of or for property or benefits received, retained, or appropriated.

350. Defendants' data mining activity in California has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

351. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

352. Defendants have not appropriately compensated AT&T for providing this benefit.

353. As a result, Defendants must make restitution to AT&T in an amount to be determined at trial. Upon information and belief, the amount of restitution to which AT&T is entitled exceeds $93,000.

**COUNT XXXVI**
**UNJUST ENRICHMENT – MISSOURI COMMON LAW**

354. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 353 above as if fully set forth herein.

355. Under Missouri law, no person may retain a benefit conferred upon him in circumstances in which retention of that benefit without paying its reasonable value would be unjust.

356. Defendants' data mining activity in Missouri has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

357. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

358. Defendants have not appropriately compensated AT&T for providing this benefit.

359. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $181,000.

**COUNT XXXVII**
**UNJUST ENRICHMENT – NORTH CAROLINA COMMON LAW**

360. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 359 above as if fully set forth herein.

361. Under North Carolina law, no person may retain a non-gratuitous benefit conferred by another without paying for its reasonable value.

362. Defendants' data mining activity in North Carolina has caused AT&T to provide them with the benefit of unauthorized access to its and other telecommunications providers' CNAM databases.

363. Defendants knowingly and willingly accepted this benefit by mining the CNAM data that AT&T provided for each call.

364. Defendants have not appropriately compensated AT&T for providing this benefit.

365. As a result, Defendants have been unjustly enriched in an amount to be determined at trial. Upon information and belief, the amount of such unjust enrichment exceeds $82,000.

**COUNT XXXVIII**
**COMPUTER FRAUD AND ABUSE – 18 U.S.C. § 1030**

366. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 365 above as if fully set forth herein.

367. Defendants engaged in interstate communication to intentionally access and obtain information from a protected AT&T computer without authorization.

368. In addition, knowingly and with intent to defraud, Defendants accessed a protected AT&T computer without authorization and obtained valuable access to AT&T's and other telecommunications providers' CNAM databases.

369. In addition, Defendants intentionally accessed a protected AT&T computer without authorization, and as a result of such conduct, recklessly caused damage and loss to AT&T's switched telephone network.

370. In addition, Defendants knowingly and without authorization caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage to a protected AT&T computer.

371. Such conduct has caused loss to AT&T that exceeds $5,000 in value during any one-year period. In addition, upon information and belief, the total amount of damages and/or loss incurred by AT&T as a result of Defendant's activity described in Count XXXVIII exceeds $1,538,000.

**COUNT XXXIX**
**THEFT BY DECEPTION – TEX. CIV. PRAC. & REMEDIES CODE § 134.005**

372. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 371 above as if fully set forth herein.

373. Texas law provides a private right of action on behalf of victims of theft. Tex. Civ. Prac. & Remedies Code § 134.005. Under Texas law, a person commits statutory theft if he unlawfully appropriates property with the intent to deprive the owner of it. Tex. Penal Code § 31.03(a).

374. "Property" includes intangible personal property. *Id.* § 31.01(5)(B).

375. Appropriation of property is unlawful if it is without the owner's effective consent. *Id.* § 31.03(b)(1). Consent is not effective if induced by deception. *Id.* § 31.01(3)(A).

376. Defendants' fraudulent spoofing of telephone numbers in the State of Texas for the purpose of misappropriating AT&T's CNAM information constitutes theft by deception in violation of the Texas Penal Code.

377. As a result of Defendants' activity described in Count XXXIX, AT&T has suffered damages in excess of $365,000.

**COUNT XL**
**BREACH OF COMPUTER SECURITY – TEX. CIV. PRAC. & REMEDIES § 143.001**

378. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 377 above as if fully set forth herein.

379. Texas law provides a private right of action on behalf of anyone who is injured or whose property has been injured as a result of a knowing or intentional commission of a computer crime. Tex. Civ. Prac. & Remedies § 143.001(a).

380. Under Texas law, a person commits the crime of breach of computer security by "knowingly access[ing] a computer, computer network, or computer system without the effective consent of the owner." Tex. Penal Code § 33.02(a). Consent is not effective if induced by deception. *Id.* § 33.01(12)(A). Breach of computer security is a felony in the first degree if in committing the offense the actor "knowingly obtains a benefit, defrauds or harms another" in excess of $20,000. *Id.* § 33.02(b).

381. By engaging in data mining with services purchased from AT&T in the State of Texas, Defendants have knowingly and intentionally accessed AT&T's computer network without effective consent, in violation of Tex. Penal Code § 33.02. In doing so, Defendants have defrauded and harmed AT&T, and have knowingly obtained a benefit as a result.

382. As a result of Defendants' activity described in Count XL, AT&T has suffered damages in excess of $365,000.

**COUNT XLI**
**COMPUTER DATA THEFT – CAL. PENAL CODE § 502(e)**

383. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 382 above as if fully set forth herein.

384. Cal. Penal Code § 502(e) creates a civil cause of action against any person who "(2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network . . ." *See* Cal. Penal Code § 502(c).

385. Under § 502(c), "data" means "a representation of information, knowledge, [or] facts." Data may be "in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b).

386. AT&T's CNAM database is stored in a computer, and the customer name information stored on the database is "data" within the meaning of § 502(c).

387. By engaging in CNAM data mining using services purchased from AT&T in California, Defendants have repeatedly, knowingly, and without permission accessed AT&T's computer network, and have taken and copied data from AT&T's computer network, in violation of Cal. Penal Code § 502(c).

388. AT&T has been injured as a result of Defendants' violations of § 502(c). AT&T's damages resulting from Defendants' violations of § 502(c) are in excess of $14,000.

**COUNT XLII**
**COMPUTER-RELATED OFFENSES – C.G.S.A. § 52-570b**

389. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 388 above as if fully set forth herein.

390. Connecticut General Statute § 52-570b creates a private right of action in favor of any person aggrieved or injured by the commission of a computer-related offense. C.G.S.A. § 52-570b(a), (c).

391. Under Connecticut law, the computer-related offense of unauthorized access to a computer system occurs when, "knowing that he is not authorized to do so, [a person] accesses or causes to be accessed any computer system without authorization." C.G.S.A. § 53a-251(b).

The computer-related offense of misuse of computer system information occurs when, "(1) [a]s a result of his accessing or causing to be accessed a computer system . . . [a person] intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization . . . takes data intended for use by a computer system, whether residing within or external to a computer system, or . . . intercepts . . . data residing within a computer system; or (3) he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection." C.G.S.A. § 53a-251(e).

392. By engaging in CNAM data mining as described in this Complaint, Defendants have repeatedly, knowingly, intentionally, and without permission accessed AT&T's computer database located in Connecticut and have taken and copied data from AT&T's computer system, in violation of § 53a-251(b) and (e).

393. AT&T has been injured as a result of Defendants' violation of § 53a-251(b) and (e). AT&T's damages resulting from Defendants' violation of § 53a-251(b) and (e) are in excess of $5,771,000.

**COUNT XLIII**
**COMPUTER CRIME – C.G.S.A § 53-452(a)**

394. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 393 above as if fully set forth herein.

395. Connecticut General Statute § 53-452(a) creates a private right of action in favor of any person aggrieved or injured by the commission of a computer crime. C.G.S.A. § 53-452(a).

396. Under Connecticut law, the computer crime of unauthorized use of a computer or computer network occurs when "any person . . . use[s] a computer or computer network without authority and with the intent to . . . (6) [m]ake or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data . . . residing in, communicated by or produced by a computer or computer network . . . ." C.G.S.A. § 53-451(b).

397. By engaging in CNAM data mining as described in this Complaint, Defendants have repeatedly, knowingly, intentionally, and without permission used AT&T's computer network located in Connecticut and have taken and copied data from AT&T's computer network, in violation of § 53-451(b).

398. AT&T has been injured as a result of Defendants' violation of § 53-451(b). AT&T's damages resulting from Defendants' violation of § 53-451(b) are in excess of $5,771,000.

**COUNT XLIV**
**ILLINOIS CABLE PIRACY ACT – 720 ILCS 5/16-21**

399. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 398 above as if fully set forth herein.

400. Illinois law creates a private right of action in favor of any person who is aggrieved by the unlawful use of a communication service or communication device. 720 ILCS 5/16-21.

401. Under Illinois law, a person commits an offense if he or she knowingly "(1) obtains or uses a communication service without the authorization of . . . the communication service provider; . . . [or] (3) modifies, alters, programs or reprograms a communication device .

. . to conceal . . . from any communication service provider . . . the existence or place of origin or destination of any communication." 720 ILCS 5/16-19.

402. Under section 5/16-19, "communication service provider" includes "any person or entity providing any communication service, whether directly or indirectly, as a reseller, including, but not limited to, a cellular, paging or other wireless communications company or other person or entity which, for a fee, supplies the facility, cell site, mobile telephone switching office or other equipment or communication service . . . ." 720 ILCS 5/16-18. "Communication device" includes "any type of instrument, device, machine, or equipment which is capable of transmitting, acquiring, decrypting, or receiving any telephonic, electronic, data, Internet access, audio, video, microwave, or radio transmissions, signals, communications, or services . . . ." *Id.*

403. By engaging in CNAM data mining in Illinois, Defendants have knowingly and intentionally obtained and used AT&T's communication services without its authorization, in violation of section 5/16-19(1). Furthermore, Defendants' fraudulent spoofing of telephone numbers for the purpose of misappropriating AT&T's CNAM information constitutes a violation of section 5/16-19(3).

404. AT&T has been injured as a result of Defendants' violation of section 5/16-19. AT&T's damages resulting from Defendants' violation of section 5/16-19 are in excess of $100,000.

**COUNT XLV**
**COMPUTER DATA THEFT – GA. CODE § 16-9-93(g)**

405. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 404 above as if fully set forth herein.

406. Georgia Code § 16-9-93(g) creates a private right of action in favor of any person whose property is injured by the commission of a computer theft or any other computer crime.

407. Under Georgia law, computer theft occurs when a person uses a computer or computer network with knowledge that such use is without authority or with the intention of "(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; (2) Obtaining property by any deceitful means or artful practice; or (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property." Ga. Code § 16-9-93(a).

408. Georgia law also prohibits invasions of privacy by means of a computer, which is committed by "[a]ny person who uses a computer or computer network with the intention of examining any . . . personal data relating to any other person with knowledge that such examination is without authority." Ga. Code § 16-9-93(c). For purposes of this section, use of a computer or computer network is "without authority" if it "exceeds any right or permission granted by the owner of the computer or computer network." Ga. Code § 16-9-92(18).

409. By engaging in CNAM data mining in Georgia, Defendants have repeatedly, knowingly, intentionally, and without permission accessed AT&T's computer system, and have taken and copied data from AT&T's computer system, in violation of § 16-9-93(a). Furthermore, in doing so Defendants have examined personal, confidential and nonpublic AT&T subscriber information, with knowledge that such examination was without authority, in violation of § 16-9-93(c).

410. AT&T and its customers have been injured as a result of Defendants' violations of § 16-9-93(a) and (c). AT&T's damages as a result of Defendants' violations of § 19-9-93(a) and (c) are in excess of $2,824,000.

**COUNT XLVI**
**TENNESSEE PERSONAL AND COMMERCIAL COMPUTER ACT OF 2003 – TENN. CODE ANN. § 39-14-604(a)**

411. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 410 above as if fully set forth herein.

412. Tennessee Code Annotated § 39-14-604(a) creates a private right of action in favor of anyone whose person or property is injured by a violation of the Tennessee Personal and Commercial Computer Act of 2003.

413. A person violates the Tennessee Personal and Commercial Computer Act if he or she "knowingly . . . accesses, causes to be accessed, or attempts to access any telephone system, telecommunications facility, computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of . . . (1) "[o]btaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises . . . ." Tenn. Code Ann. § 39-14-602(a). A person also violates the Act if he or she "intentionally and without authorization, directly or indirectly . . . (5) [m]akes or causes to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network . . . ." *Id.* § 39-14-602(b).

414. By engaging in CNAM data mining in Tennessee, Defendants have repeatedly, knowingly, intentionally, and without authorization accessed AT&T's computer network by means of false or fraudulent pretense, and have made unauthorized copies of data from AT&T's computer network, in violation of Tenn. Code Ann. § 39-14-602(a) and (b).

415. AT&T has been injured as a result of Defendants' violations of § 39-14-602. AT&T's damages as a result of Defendants' violations of § 39-14-602 are in excess of $66,000.

**COUNT XLVII**
**TAMPERING WITH COMPUTER DATA – MO. REV. STAT. § 537.525**

416. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 415 above as if fully set forth herein.

417. Missouri Revised Statute § 537.525 creates a private right of action in favor of the owner or lessee of a computer system, computer network, computer program, computer service or data against any person who commits the crime of tampering with computer data. Mo. Rev. Stat. § 537.525.

418. Under Missouri law, tampering with computer data occurs when a person, "knowingly and without authorization or without grounds to believe that he has such authorization . . . (3) [d]iscloses or takes data, programs, or supporting documentation, residing or existing internal or external to a computer, computer system, or computer network; . . . (5) [a]ccesses a computer, a computer system, or a computer network, and intentionally examines information about another person; [or] (6) [r]eceives, retains, uses, or discloses any data he knows or believes was obtained in violation of this subsection." Mo. Rev. Stat. § 569.095.

419. By engaging in CNAM data mining in Missouri, Defendants have repeatedly, knowingly, intentionally, and without permission accessed AT&T's computer network, and have thereby examined, taken, and retained personal, confidential and nonpublic AT&T subscriber information, in violation of § 569.095.

420. AT&T and its customers have been injured as a result of Defendants' violations of § 569.095. AT&T's damages as a result of Defendants' violations of § 569.095 are in excess of $21,000.

**COUNT XLVIII**
**COMPUTER TRESPASS – N.C. GEN. STAT. § 14-458(c)**

421. Plaintiffs reallege and incorporate by reference the allegations of paragraphs 1 through 420 above as if fully set forth herein.

422. North Carolina General Statute § 14-458(c) creates a private right of action in favor of anyone who is injured by the commission of a computer trespass.

423. Under North Carolina law, a computer trespass occurs when anyone uses a computer or computer network without authority and with the intent to "[m]ake or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network." N.C. Gen. Stat. § 14-458(a)(5).

424. By engaging in CNAM data mining in North Carolina, Defendants have repeatedly and without authorization used AT&T's computer network to copy computer data residing in and communicated and produced by that network, in violation of § 14-458(a)(5).

425. AT&T has been injured as a result of Defendants' violations of § 14-458(a)(5). AT&T's damages as a result of Defendants' violations of § 14-458(a)(5) are in excess of $95,000.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs request that the Court enter judgment in favor of the Plaintiffs, and against all Defendants, jointly and severally, awarding Plaintiffs:

a. Actual damages in an amount to be determined at trial;

b. Punitive damages to deter Defendants from further unlawful conduct; and

c. Plaintiffs' costs, including attorneys' fees, incurred in connection with this action.

In addition, Plaintiffs further request the Court to enter an order permanently enjoining the Defendants, and each of them, from engaging in, facilitating, or assisting any fraudulent spoofing of telephone numbers not issued to them for the purpose of engaging in CNAM data mining as described in this Complaint.

Dated: August 26, 2011

Respectfully Submitted,

Southwestern Bell Telephone Company; AT&T Communications of Texas, Inc.; Indiana Bell Telephone Company d/b/a AT&T Indiana; Pacific Bell Telephone Company d/b/a AT&T California; BellSouth Telecommunications, LLC; Teleport Communications Group, Inc. d/b/a TCG Illinois; New Cingular Wireless PCS, LLC d/b/a AT&T Mobility; and SNET Diversified Group, Inc. d/b/a AT&T Diversified Group

By: /s/ Lawrence Fogel
Lawrence Fogel

Richard M. Parr
State Bar No. 15534250
Lawrence Fogel
State Bar No. 24050608
AT&T Services, Inc. – Legal Department
One AT&T Plaza, Suite 2900
208 South Akard Street
Dallas, Texas 75202-4208
(214) 757-3386
(214) 748-1660 (fax)
rp3639@att.com
lf143c@att.com

**OF COUNSEL**:

Christian F. Binnig (IL Bar No. 6194161)
Jeffrey M. Strauss (IL Bar No. 6181435)
Matthew D. Provance (IL Bar. No. 6300603)
MAYER BROWN LLP
71 South Wacker Drive
Chicago, IL 60606-4637
(312) 782-0600
(312) 701-7711 (fax)
cbinnig@mayerbrown.com
jstrauss@mayerbrown.com
mprovance@mayerbrown.com